Your Complete Prep Guide to Cybersecurity in 2021 and Beyond

Ensuring you and your business can fully prevent and resolve any security issues

White Paper

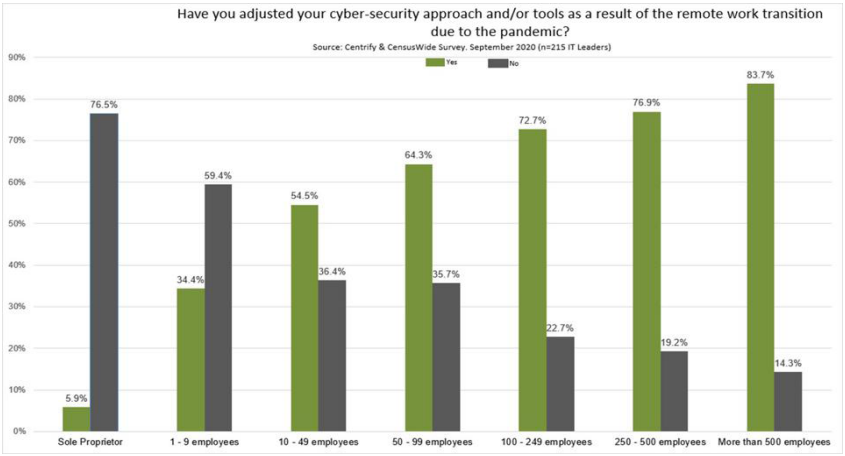
CRA™
Transform IT
Computer Resources of America

Introduction

Of the many lasting impressions inflicted by the COVID-19 pandemic, the world has seen the recent creation of a hotbed for threat actors and hackers, which is greatly affecting the current state of cybersecurity in 2021.

At the beginning of the pandemic, more than a year ago now, various businesses viewed the work-from-home shift as temporary, with many organizations adopting long-term plans to gradually filter back into the office setting. So, they responded accordingly, doing everything possible to improve temporary remote working conditions.

However, this shift to virtual work exponentially increased the risks and threats to an organization's cybersecurity infrastructure. The biggest culprit in this, an individual's home network which lacks the defensive capabilities of a large business network. As a result, personal computers are much more vulnerable than company-managed and issued equipment. Given the situation, 83% of big organizations and some 60% of small and medium corporations transformed their cyber-security approach.



Source: 83% Of Enterprises Transformed Their Cybersecurity In 2020

The Shift in Cyberattacks

Today, it seems that the government and businesses were correct in preparing for a long-term evolution in the cybersecurity landscape. For example, 52% of companies claimed they had seen a sharp rise in cyberattacks, especially ransomware and hacking, since they moved to remote working near the start of the pandemic.

It's estimated that cyberattacks, particularly ransomware attacks, will happen every 11-seconds in 2021, according to Cybercrime Magazine. Cyber crime increased by 600% due to the pandemic in 2020, and ransomware is emerging as a leading cybersecurity threat in 2021.

In the midst of this cyber-evolution, what should businesses do to defend their data, profits, and serenity? This whitepaper will look deeply into the top cybersecurity threats in 2021 that businesses commonly face, and will provide effective ways to tackle them.

Threat Report

Cybersecurity defenses were taken aback during the first quarter of 2021 by cybercriminals ready to exploit even the tiniest crack in protections to ravage invaluable assets.

By mid-2021, cybersecurity risks and threats from all sides closed in, taking with them upgraded techniques and higher motivation to impact targeted industries.

These security threats include high-profile Covid-19-related scams, ransomware attacks, critical vulnerabilities, active campaigns, and other threats.

Here's a list of cybersecurity 2021 threats to look out for:

Ransomware

Modern ransomware attacks continue to pose significant threats to government sectors and businesses of all sizes. It's amongst the most prevalent cyber threats globally, with above 7-million combined URL, file, and email threat detections. Additionally, the threat actors shifted aggressively and quickly with assaults on key sectors like banking, manufacturing, and government.

In 2021, cybercriminals have adopted sophisticated technologies. In addition, they have taken more advanced business models to create stealthy and efficient ransomware attacks. This new series of attacks have distinctive features such as data exfiltration instead of simple encryption, secret online collaboration, prolonged usage of an affiliate program, and APT victim targeting, and more.

Most prominently, during the first six months of 2021, ransomware actors were seen successfully extracting invaluable data and extorting companies using the double-extortion technique.

Ransomware attacks worldwide rose

350%

in 2018.

Source: 2021 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends

In addition to demanding ransom against decrypting valuable data, assailants placed increased pressure on their targets by threatening to release confidential data on leak sites. Enterprises holding valuable intellectual properties view these attacks as a grave concern. Data breaches come with lawsuits, reputational damage, and regulatory penalties.

Apart from that, the report also saw a rise in "Distributed Denial-of-Service (DDoS)" attacks along with "Quadruple Extortion Models" to harass clients and raise their chances of payment.

Advanced Persistent Threats (APTs)

Compared to ransomware attacks, Advanced Persistent Threats (APTs) are relatively uncommon for many organizations. However, due to their complexity and severity, APTs can be far more damaging to companies and governmental organizations.

APTs are covert campaigns targeting particular groups and utilize sophisticated technologies and malware to persist and infiltrate the victims' system. The objectives differ for every operation, and can include the theft of invaluable user data, stealing financial records, and much more.

The APT threat increased exponentially in the first few months of 2021. For example, these groups have updated their toolkits and broadened target bases, focusing on covert infiltration methods and seeking new means to abuse authorized systems and tools to conduct malicious actions.

In addition, they continued searching for and exploiting vulnerabilities in commonly used business tools such as AWS cloud-server, Kubernetes, and prevalent email platforms. Nevertheless, spear-phishing is still the most successful and prevalent way for APT attackers to make their way into a victims' system.

COVID-19 Scams

Even during the pandemic, it's business-as-usual for many cybercriminals as they continue unchaining new and modern threats along with refurbishing the existing ones. Some threat actors took advantage of the outbreak using distress and uncertainty caused by this situation.

COVID-19-Related Risks

As the COVID-19 vaccination drive is ongoing across the world, threats associated with its vaccine also surged. This involves malicious files, text messages, phishing pages, misinformation sites, and emails. The common targets of such scams include but are not limited to telecommunication, retail, finance, government, and banking sectors.

Active Threats

XCSSET malware affects Xcode projects and victimizes Mac users. In 2021, cybercriminals upgraded this malware with features unmatched that allow it to adapt to x86_x64 and ARM64 Macs. XCSSET can also harvest sensitive data from various websites, including crypto-currency trading platforms.

PandaStealer is yet another new data stealer capable of collecting sensitive data such as records of previous transactions and private keys from victims' digital wallets.

Additionally, it can harvest personal data from numerous other applications, exfiltrate information from browsers, and take screenshots. This malware is primarily propagated via spam emails requesting business quotes.

COVID Scams & Other Vulnerabilities

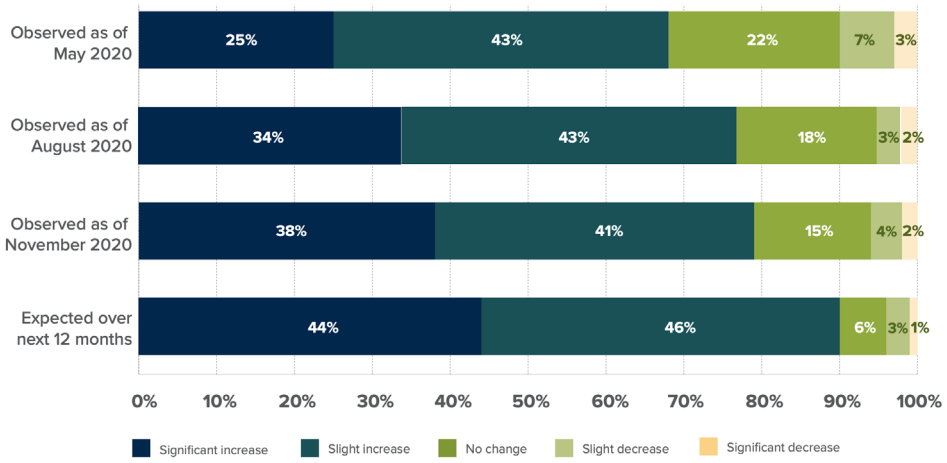
Protect Against XCSSET: To protect your systems from this kind of cybersecurity menace, users should download applications from legitimate and official marketplaces. Apart from that, businesses can also consider multi-layered security solutions capable of providing multi-device protection and comprehensive security against XCSSET malware.

Protect Against PandaStealer: To secure systems from file-less threats using spam emails as vectors, businesses can utilize endpoint solutions for protecting users and their employees from risks by detectingspammed messages and malicious files along with associated malicious URLs.

Other Vulnerabilities

A few other notable vulnerabilities have also made headlines in 2021 as various researchers rushed to patch impacted systems before they could pose risks and upset work setups, including virtual ones.

Change in overall level of fraud



Source: Fraud in the Wake of COVID-19: Benchmarking Report

Here are some significant vulnerabilities:

ProxyLogon

ProxyLogon is a general term for “CVE-2021-26855,” a vulnerability on “Microsoft Exchange Server,” allowing cybercriminals to bypass the authentication process and impersonate as admin.

Microsoft SharePoint

About five “Remote Code Execution (RCE)” susceptibilities also impacted Microsoft SharePoint – an online storage and document management platform, which one can utilize in virtual work setups as well.

VPN Vulnerabilities

As work-from-home setup continues in most sectors, VPN or Virtual Private Networks remains a vital tool for guaranteeing security for your information. Unfortunately, attacks on these vulnerabilities continue to grow with time.

PrintNightmare

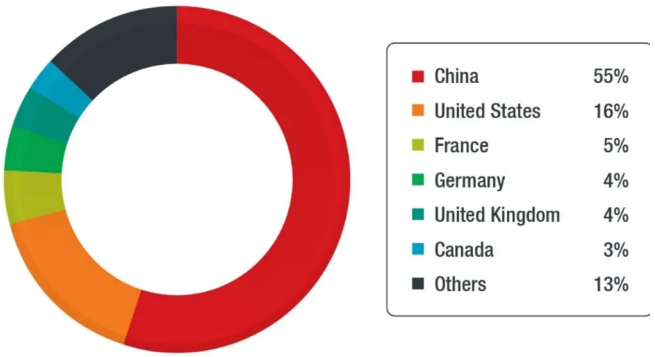
PrintNightmare is a term for "CVE-2021-1675" – a critical 'Windows Print Spooler' vulnerability allowing arbitrary code execution in addition to system-level privileges. Overall, vulnerability detection cases have shown a slight decline in the first few months of 2021, with a prominent decrease in significant vulnerabilities.

Cloud And IoT

Circumstances that arose from the outbreak pushed businesses of all sorts to adopt virtual systems backed by technologies like IoT and Cloud. But even these domains have their own share of risks and threats.

The percentage of servers compromised per country.

Source: TeamTNT Targets Kubernetes



Cloud

In 2021, some significant threats include TeamTNT assaults. From the outset of this year, there were numerous incidents where TeamTNT actors targeted cloud systems. Here are a few examples:

- *AWS Credentials:* These threat actors had stolen AWS credentials via a binary holding 'hard-coded shell script.' As a result, more than 4000-instances were endangered.
- *Kubernetes Clusters:* TeamTNT has also endangered Kubernetes clusters at large as far as 50000 IP addresses got affected across several groups.
- *The IoT:* Not just the cloud, 2021 has also witnessed risks in the IoT, including "5G," "routers," and "Long Range Wide Area Network (LoRaWAN)."
- *LoRaWAN:* Although LoRAWAN devices benefit intelligent cities and enterprises, they aren't immune to risks and cyber threats. Threat actors have found several exploitable vulnerabilities in them.
- *5G:* Establishing 5G networks for businesses come with hazards that cybercriminals can easily damage in numerous ways, including MQTT hijacking, DNS hijacking, TCP/Modbus hijacking, resetting, or downloading vulnerable 'programmable logic controllers,' SIM swapping, and remote desktop.
- *Routers:* Routers have many security issues; however, the most leading threat is VPNFilter – the IoT botnet. To compromise storage devices and routers, VPNFilter employs exploits and backdoor accounts.

Ways To Protect Against Leading Cybersecurity Threats

Cybersecurity threats are constantly evolving, and the risks aren't diminishing as well. In fact, according to one report from Accenture, businesses all over the world now confront 22-security breaches every year, on average.

Given the nature of assaults, every enterprise should have a cyber attack prevention plan in place.

How To Defend Against Ransomware

There are various ways businesses can protect their sensitive information from ransomware assaults. Here are a few valuable ways you can use to keep ransomware attacks at bay:

- Train your employees to identify phishing attacks
- Back your files frequently and routinely
- Practice the principle of exclusive access
- Keep all software programs, including operating system up-to-date
- Never pay ransom unless necessary
- Disable features such as auto-run, virtual desktop connections, macro content (Microsoft Office), etc.

How To Protect Against APTs

Defending against APT threats requires a multi-layered approach. Here's how you can protect against such kinds of attacks:

1. Develop A Multi-Layered Approach

An effective defense requires controlling all aspects of a network via up-to-date tools such as Next-Generation firewalls, antivirus software, endpoint protection, software patching, SIEMs, identity, and authentication management. Every security layer provides another hindrance for APTs that are constantly evolving to remain hidden for long. When developing a multi-layered approach, keep your emphasis on prevention because it's easier to avoid assaults rather than responding to them. This way, your system will remain cleaner and provide your SIEM equipment a chance to fight against APT attacks.

2. Ensure Rigorous Monitoring

Mainly, access requests and logins should be routinely checked so that anomalies can easily be spotted and solved quickly.

3. Allow List Applications

While some users may find it annoying and frustrating, allowing listing applications ensures forced installations are recognized timely.

4. Utilize Threat-Intelligence Services

They use basic information on emerging risks to offer businesses actionable data. When merged with endpoint protection and next-generation software, this data allows organizations and businesses to uncover cybersecurity risks quicker.

Other Forms Of Cybersecurity Preparedness

Here are a few other cybersecurity preparedness steps that businesses should take no matter the cost:

1. Audit Your Cyber-Preparedness

This will help you understand the multi-layered potential for cyber-security vulnerabilities fully. Assailants often hit secondary targets like medium-security devices such as networks (employees working from home), medical devices or printers, supply-chain members, and endpoints.

2. Promote A Cybersecurity Culture

It's pretty common to confront customers and employees for underutilizing proper security measures, so educate them accordingly. For example, establish best practices such as multi-factor authentication. Additionally, train your staff members to determine email phishing. Also, ensure everyone has a solid password.

3. Provide Multi-Factor Authentication

The threat attackers have become experts at stealing people's log-in credentials. They are able to convince the savviest employees into clicking phishing emails. Providing a multi-factor authentication process means cybercriminals will be short on factors and won't get access to information and data.

4. Stay Updated On Security Upgrades And Updates

Remember, no matter how big, cybercrime is always avoidable. Though security upgrades may look mundane, they aren't. For example, Microsoft has detected security susceptibility capable of putting your business data and servers at risk. Now, the immediate step should be to install that vital security patch and avert the threat.

Work With Computer Resources of America

As 2020 saw companies shifting towards remote working, it also witnessed a sudden increase in cybersecurity attacks ranging from ransomware, hacking, and more.

These attacks became much more advanced in 2021, as large private corporations and government bodies confronted numerous assaults from threat actors.

Make your company safe and secure from cybersecurity attacks and threats! We can help you transform your business and make it threat-free with our comprehensive technology solutions. Our services include managed IT, cloud computing, IT consulting, staffing, and more!

Get the expert assistance you need. For more information, please contact us today.

CRA™ Transform IT
Computer Resources of America

Corporate Headquarters

729 7th Avenue, New York, NY 10019 – 212-376-4040 – www.consultcra.com – hello@consultcra.com

©2021 Computer Resources of America. All rights reserved.